Strategy Research Project

PROTECTION: THE KEY TO CYBERSPACE

BY

MR. LEROY LUNDGREN
Department of Army Civilian

USAWC CLASS OF 2010

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College, Carlisle Barracks, PA 17013-5050

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **30 MAR 2010**	2. REPORT TYPE	3. DATES COVERED

4. TITLE AND SUBTITLE **Protection: The Key to Cyberspace**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **LeRoy Lundgren**	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College ,122 Forbes Ave.,Carlisle,PA,17013-5220**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
see attached

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE		**34**	
unclassified	**unclassified**	**unclassified**			

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

PROPERTY OF U.S. ARMY

USAWC STRATEGY RESEARCH PROJECT

PROTECTION: THE KEY TO CYBERSPACE

by

Mr. LeRoy Lundgren
Department of Army Civilian

Mr. William O Waddell
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Mr. LeRoy Lundgren

TITLE: Protection: The Key to Cyberspace

FORMAT: Strategy Research Project

DATE: 12 March 2010 WORD COUNT: 6,787 PAGES: 34

KEY TERMS: Information Assurance, Security Tools and Standards, Threat

CLASSIFICATION: Unclassified

The Department of Defense, as well as the United States, is dependent upon "reliable information and communications networks and assured access to cyberspace", in order to conduct successful military operations and to ensure the economic viability of the nation. The increasingly sophisticated actions of state and non state actors are impacting cyberspace to the point that one must question the viability of ensuring an acceptable degree of reliability and access. It is an international issue, yet the international community cannot reach a consensus on how to develop a common set of laws and or treaties that will force state and non state actors to operate in a predictable manner. The hardware, software and firmware that make up network and security tools are suspect and often riddled with vulnerabilities. A mechanism for establishing and enforcing enterprise standards, policies and procedures, does not exist. Since all participants in cyberspace are interconnected, the most effective participant is often forced to the level of the lowest common denominator. The DoD, as well as the nation must start making fundamental changes in how cyberspace is governed and enforcing standards that must be met.

PROTECTION: THE KEY TO CYBERSPACE

> There is no exaggerating our dependence on the Department of Defense (DoD) information networks for our command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field. In the 21st century, modern armed forces simply cannot conduct high-tempo, effective operations without, reliable information and communications networks and assured access to cyberspace. [1]

The United States and the global economic and trading system are dependent upon the use of cyberspace to function efficiently. If information and the information technology (IT) infrastructure that make up cyberspace cannot be adequately protected then our national and global economic well being, social progress and security are at risk. It is generally accepted that the amount of resources and restrictive nature of policies that would be necessary to provide protection against all and any intrusions would negate the utility of the cyber domain. Since there are limited resources and reluctance, if not inability, to function in cyberspace with highly restrictive policies, it is generally accepted that a “persistent threat” will always exist inside of the IT infrastructure. [2] Thus it will be important to not only protect against intrusions from outside the IT infrastructure, it will be equally important to have the capability to detect intrusions “inside the wire” and to recover in a manner proportionate to the degree of risk incurred. In general (there are always exceptions), neither the DoD nor the nation have taken the necessary steps to provide more than a static defense dependent upon layers of hardware, firmware and software that in many cases fail to meet adequate security standards. The majority of elements within the DoD, national, and international global information grid do not operate in unison or share information to the degree that is necessary to defend against an adversary that is increasingly sophisticated and conducting global attacks. The definitions, laws and treaties that support or define the type of intrusive/illegal cyber activity that criminal elements and other non state and nation state actors perpetuate, is inadequate to provide the basis for successfully defending against or prosecuting illegal/intrusive activity to the degree necessary to facilitate an adequately functioning cyberspace.

Despite the interest in the development of tools and organizations able to conduct attacks against and exploit the IT infrastructure in cyberspace, the fact remains that the key to cyberspace will be the ability to provide an adequate cyberspace protection posture. The intent of this paper is to discuss relevant aspects of the current cyberspace environment so as to make recommendations as to what should be done to develop an adequate cyberspace protection posture.

Cyberspace Environment

The first recommendation is that the entire nation must be educated about the persistent conflict in cyberspace and what is at stake. The nature of the conflict in cyberspace requires the active participation of the private and public sector, and cannot be limited to the government or military. Private industry and the everyday citizen must execute an active role in order to develop and maintain an adequate cyberspace protection posture.

On a daily basis there are reports of information and information infrastructures in cyberspace being compromised and personal information, account numbers, passwords, industry intellectual property, banking and financial funds being exploited /stolen for fraudulent/hostile reasons.   Governmental and industry reports are constantly describing a threat that is becoming more sophisticated, more difficult to protect against and is spreading to all sectors of our nation, private as well as public. [3]

Cyber is the term used to describe these types of activities and cyberspace is the term used to "describe an interdependent network of information technology infrastructures that supports and facilitates the processing, transporting and storage of information". [4] What is most distressing is that the chaotic environment described above is mainly a result of organized criminal effort. [5] There is a great deal of discussion about the potential of offensive actions such as attack and exploit being used in cyberspace. [6] The concept of conducting an active defense (includes cyber attack and exploitation) may result in a de-emphasis on what is often referred to as a passive defense (protection aspect of cyber). The protection of information and IT infrastructures must remain a priority. A cyber attack and exploit capability may enable the U.S. to develop a degree of deterrence, but it does not provide an adequate protection posture able to protect against the attacks (criminal/exploitation) that are already being executed. Without an adequate protection posture the current cyberspace environment is undesirable and unsustainable.

No matter what degree of protection that can be achieved, it will be essential for any nation or non nation state actor to understand how to operate in a hostile cyber environment. There is evidence that illegal/unauthorized cyberspace activity will be used as a tool to conduct criminal activity and as a weapon on the 21st century battlefield. The scope of the cyber battlefield will extend beyond the military realm and include critical governmental and nongovernmental economic, political and financial targets. [7] The participants of a cyber battlefield will include private citizens as willing, and more often than not, unwilling participants.

In 2008 the Bush administration published The National Strategy to Secure Cyber space. [8] This was the first national level strategy document published on this subject. This document articulates what the general public views as a relatively new and unique phenomenon, rather than the increasingly sophisticated challenge that has been developing for almost two decades. The strategy states that “the way business is transacted, government operates, and national defense is conducted have changed. These activities now rely on an interdependent network of information technology infrastructures called cyberspace”. [9] These words make it clear that this challenge is real, and if not adequately met would impact negatively upon the vital if not survival interests of the United States. The National Strategy to Secure Cyber Space document further states that this “extraordinary difficult strategic challenge requires a coordinated and focused effort from the entire society – the federal government, state and local governments, the private sector, and the American people”. [10] While the public expects the government to be involved in conflict, the public is not accustomed to the fact that private industry and the American citizen will need to be aware of the cyber environment and become active participants supporting governmental efforts to protect information and information technology infrastructures. While it is clear that private industry is and will continue to be a target, based on the fact that the private industry owns the majority of the national and international information technology infrastructure, it is not clear what role private industry will play. Should industry strike back against attackers? [11] To what degree will private industry have to coordinate with governmental agencies? When does the sharing of information violate privacy laws?

The American citizen will be a cyber target, and the citizen will not be accustomed to the fact that they will need to step up and provide adequate security for their private computer equipment in order to preclude their assets being used as an attack platform. There are examples of private computer resources being infected with hostile code and therefore unwittingly becoming part of a robot network (BOTNET) whose purpose is to conduct cyber attacks. [12]

The Obama administration completed and published an assessment of the Bush administration cyber policies and strategy. [13] The assessment acknowledged that while "efforts over the past two years started key programs and made great strides by bridging previously disparate agency missions, they provide an incomplete solution". [14] The review reiterates: (1) No federal agency by itself can provide a solution, (2) There must be a real partnership between the private and public sector since the majority of the national and international IT infrastructure is in the private sector, (3) There needs to be a serious awareness and educational push to insure that American people understand what is at stake, and (4) The leadership must come from the top". [15] Yet, it would appear that the level of concern and the degree of risk that is posed to the nation has not translated into the allocation of resources to support cyber initiatives that would seem commensurate with the vital interest that are at stake. The Obama administration appointed Howard Schmidt as the Cyber Coordinator almost one year into his administration. [16] It will be interesting to see what power Mr. Schmidt will have since his position title includes the term "coordinator". The United States has been faced with significant issues such as a threatened global financial "meltdown", the ongoing wars in Iraq and Afghanistan, the threat of Iran becoming a nuclear power, concern with what

North Korea will do with their nuclear technology knowledge, and the ongoing focus on domestic issues such as healthcare reform. If a casual observation considers the justifiable preoccupation with non cyber events, and the fact that no cyber attacks against targets in the United States have led to long term and wide spread disruption, it may be understandable why protecting cyber space has not been a priority. It is unfortunate that it will probably take a Cyber disaster before the nation will seriously address the need to develop an adequate cyberspace protection posture.

It is difficult to discuss what is known about the threat to U.S information and information technology infrastructures because it is remains highly classified. McAfee's 5th annual Virtual Criminology Report stated that "based on the development of Cyber warfare capabilities and the demonstrated use of methodologies, there appears to be instances of cyber war and that perhaps a "Cyber Cold War" already exist. [17] It goes on to state that too much of what is known about potential attacks and the difference or divergence of cyber espionage and cyber war is classified, and that since industry as well as the private citizens are major stakeholders in this potential conflict that the subject needs to be discussed in public.

Without access to classified information a clear picture is evolving. The threat to cyberspace has been well documented in the press. Russian involvement with Cyber espionage was recorded in 1998 and given the code name of Moonlight Maze. [18] During Moonlight Maze there were intrusions into the Department of Defense (DoD) information technology infrastructure and significant amounts of unclassified but sensitive information was sent to servers in Russia. The United States confronted Russia about these intrusions but the Russian government denied any knowledge.

Chinese hackers gained access to DoD networks in 2005 and downloaded significant amounts of unclassified but sensitive data to locations in China. This operation was assigned the code word Titan Rain. [19] The Chinese have denied any state involvement with this activity. A clear pattern is being established. Both the Russians and the Chinese appear to be conducting offensive cyber activity through a proxy and thus are able to deny involvement. [20] One must be concerned that since this activity took place undetected, what else is happening that is undetected? What is being inserted in friendly networks that constitute the establishment of "sleeper cells" that can become active during a crisis? What makes this extremely worrisome is that "The skill sets necessary to penetrate a network for intelligence gathering purposes in peacetime are the same skills necessary to penetrate that network for offensive action during wartime." [21]

In May of 2007 Estonia was attacked. The attacks were launched from Russia but again the Russian government denied any involvement. The attacks impacted all commercial banks, telecommunication services, media outlets and key components of the information technology infrastructure such as Domain Name servers (DNS) [22] Even though the attacks eventually ended and services were restored, the event had a significant impact on the people of Estonia. "In Estonia the immediate damage to specific systems were fairly limited and rarely rose above the level of inconvenience. The second order of effects however—fear, loss of confidence in banking and communication systems and a national sense of vulnerability—could lead to even more negative enduring consequences than a limited military incursion. " [23]

In August of 2008 the country of Georgia was the target of a cyber attack that coincided with a Russian conventional military attack. [24] As a result of these attacks “the Georgian government found itself cyber-locked, barely able to communicate on the Internet. “ [25]

In December of 2009 senior defense and intelligence officials verified that an Iranian-backed insurgent group was using an off-the-shelf software program to intercept the video feeds from U.S. Predator drones. [26]

In July 2009 large scale “denial of service” attacks were executed against the republic of Korea and the United States. [27]

On 12 January 2010 it was reported that attacks originating in China hit Google and at least 34 other large U.S. corporations, as well as human rights groups and Washington-based think tanks. [28] The Chinese government is denying any involvement. When talking about Chinese offensive cyber activity, many believe that the Chinese have demonstrated that they possess a “mature and operationally proficient Computer Network Operations (CNO) capability”. [29]

China claims that the United States is the worst cyberspace offender. It is true that the majority of attacks that occur in the world come from United States internet protocol (IP) address space. Thousands of U.S. computers are compromised and are often part of BOTNETS that are used to conduct denial of service attacks and to insert malware. The Chinese expect the U.S. to start controlling the number of attacks that originate from the U.S. IP address space, before the U.S. should expect others to do the same. [30]

In summary, it is clear that the military alone cannot successfully defend against attacks in the current cyberspace environment. This conflict is real, and it will require the active participation of the federal and state governments as well the private sector and the American citizen. There must be a significant push to educate the public and to foster information sharing and joint action with private industry.

Cyber Space and Legal Norms

The United States must use all means of national influence to foster the development of treaties and laws that are enforced on a global level. Normally the existence of laws, treaties and agreements can be used to establish generally accepted norms for operating in an international or global domain such as cyberspace. Unfortunately there are not a significant number of cyber related laws or treaties that exist and the ones that do exist do not include nations that are significant actors in cyberspace. Currently "no comprehensive international treaty to regulate cyber attacks exist. " [31] In 2001 the member states of the Council of Europe and other interested states signed the European convention on Cyber Crime. [32] The United States started enforcing the convention on 1 January 2007, but China and Russia have not agreed to adopt the convention. [33] "The prevailing views of states and legal scholars are that states must treat cyber attacks as a criminal matter". There is no general agreement that a cyber attack qualifies as an armed attack and a legal response could be taken under the banner of the law of war. As previously discussed it is extremely difficult to identify the actual source of cyber attacks and the law of war requires states to attribute an armed attack to a foreign government, or its agents, before being able to legally respond with force.[34] Michael Schmidt's article on the six criteria for determining if a cyber attack would be considered an attack that may be justification for a cyber or armed response is often quoted. [35] While these criteria may one day provide the basis for determining if a cyber attack is a legal basis for going to war, the fact remains that there are many view points about whether the current Law of War can be applied to cyber attacks. [36]

After Estonia was attacked there was a great deal of discussion within the North Atlantic Treaty Organization (NATO) concerning cyber deterrence. The Estonian President, Toomas Hendrik Ilves, made a statement at the NATO summit in Bucharest that a cyber attack against a NATO nation should lead to invoking Article 5 of the NATO treaty that states an attack against one is an attack against all. Another senior NATO official stated that it was unlikely that article 5 would be the basis for a cyber issue, and yet another senior NATO official did not exclude the use of Chapter 5 provided that it was "bound to political and technical responses." [37] There is a growing awareness within NATO that there is a need for protection but there is reluctance to conduct retaliatory attacks, even when a member was obviously the target of a cyber attack.

In summary, adequate treaties and or laws do not exist that could provide an international norm that would govern cyberspace. While the European convention categorizes current offensive action in cyberspace as criminal, others are working to develop a process that would categorize this activity as an attack, and would justify an offensive conventional or cyber response.

DoD Cyber Command Initiative

Based on the fact that the current cyberspace environment posses so many risks, the DoD established a four star Cyber Command with an Initial Operational Capability (IOC) date of 1 October 2009 and a Full Operational Capability (FOC) date of 1 October 2010. [38] The intent of the Cyber Command is to address the risks posed by cyber threats and vulnerabilities. The command must be capable of "synchronizing war fighting effects across the global security environment as well as proving support to civil authorities and international partners." [39] This is a significant initiative that will not only provide the coordination necessary for the synergistic application of cyber attack, and exploitation and protection within the DoD; the command will also be responsible for supporting civil authorities and international partners. [40] It was reported that Google had reached an agreement with the National Security Agency (NSA) to solicit NSA's assistance in analyzing the major corporate espionage attack that originated from Chinese IP address space. [41] This may be the start of a forum for sharing information with industry; something that is vital to protecting cyberspace. This could result in the establishment of an industry and governmental information sharing forum that will address attacks that originate from outside the United Sates. If NSA could work with industry, and share with them what NSA knows, then perhaps NSA could become the conduit for private industry to share information; not just between one industry member and NSA, but with NSA and all members of industry that own a part of the national critical infrastructure. NSA could ensure that members of industry are not identified so as to preclude public embarrassment and any compromise of proprietary information. This could become a more efficient means of information sharing than the ad hoc arrangements that now exists.

Strategic Cultural Change

The nation, as well as the DoD need to assess what basic fundamental initiatives must be implemented so as to provide the basis for an improved cyberspace protection posture. While the following initiatives are important and address fundamental issues, they certainly are not the only initiatives that need to be taken. The nation as well as the

DoD need to develop and aggressively implement a strategic communication plan that changes the culture concerning cyberspace and in particular the defense of cyberspace.

Usually funding levels reflect the importance that is associated with a program. The amount of funding that is provided to the protection of cyberspace is best described as inadequate when compared with what is at risk. [42] In some ways the nation and the defense establishment is hesitant to commit, on a routine and continuous basis, resources that are necessary to counter the evolving and sophisticated cyber threat. The nation and the DoD must recognize that there will be a need for a continual investment in Cyberspace so as to counter the current and evolving threat.

Another aspect of culture that needs to change is how the consequences of cyber attack and exploitation are described and viewed. Cyber attacks and exploitation are discussed in intangible terms such as loss of confidence, negative perceptions, information loss, identities stolen etc. These terms do not have the impact that physical destruction, wounded warriors and death convey. Physical is real, and while most everyone agrees that cyber attack and exploitation posses significant risks, these activities have not yet resulted in any tangible physical loss or destruction. The leadership must convey a message that will help the private and public sectors to understand the importance of cyberspace to the future of the DoD and the nation.

Culture and Enterprise Implementation

There is an urgent need to change the culture of the nation and the DoD reference how best to protect information and IT infrastructures. The cyber threat cannot be defeated by multiple islands of varying protection postures. The best protection will be achieved when the entire infrastructure is defended from an enterprise perspective, enforcing a common set of adequate security standards. The nation, as well as the DoD, is composed of numerous bureaucracies. These competing bureaucracies must start to leverage enterprise solutions and not continue to implement separate enclaves consisting of different levels of security.

One of the DoD initiatives of the DoD-Wide IA/CND Enterprise Solutions Steering Group (ESSG) is the Host Based Security Solutions System (HBSS). The HBSS baseline is a flexible commercial-off-the shelf- (COTS) based application. It monitors, detects and counters known cyber threats. The HBSS solution will be eventually attached to each host (server, desktop and laptop) in DoD. The system will be managed by local administrators and configured to address known exploit traffic using an Intrusion Prevention System (IPS) and firewall. [43] This initiative is extraordinary in the sense that it is truly a DoD enterprise initiative. In gross terms the HBSS is a system of modular tool sets that each service and agency is to implement so as to provide a common set of tools/capabilities across the DoD, for monitoring and reporting information with the intention of providing a DoD enterprise IA/CND situational awareness and the ability to direct and implement DoD wide directives and policies. The HBSS initiative is suffering the usual challenges that face any enterprise implementation. To be successful there must be change in service and agency culture. There is reluctance on the part of some services and agencies to implement HBSS because it provides the DoD the ability to obtain information on the status of service and agency systems and the ability to direct configuration changes/blocks etc. via the HBSS system. The services have responded to the initiative differently over the years. [44] The Navy response has been consistent, viewing the implementation as an infringement of their duty and responsibility. The Navy felt that they had the authority and responsibility to protection Navy networks and systems. They fought hard against any reporting and data to the DoD level, only agreeing to accept DoD enterprise guidance that would impact their network security and operational network posture. The Air Force accepted the value of providing an enterprise view of their networks and even accepted that they would be directed to execute enterprise level activities that would impact their security and operational network posture. The Air Force was always at odds concerning the quality of the technology, not wanting to implement certain hardware/software items that contained perceived weaknesses. The Air Force, even though it took part in the Technical Advisory Group (TAG) that recommended the technology, always wanted to test the equipment and software separately. The Army response to this initiative has been slow and arduous.   It was hard to convince the Army senior leadership that something such as the protection of information and networks is worthy of being funded with resources that could be used for funding traditional kinetic conflicts.

Most importantly the HBSS system can support the development and fielding of a new capability as well as the modification of existing capabilities. Other capabilities that may be considered are a rouge detection module that will detect any host that is operating without HBSS, a compliance profiler that will report the patch and upgrade posture of host assets, an application blocking module, and a module that negates the majority of threats that Social Media Sites pose. A solution is available that will leverage the buying power of the enterprise, provide a solution to keeping the technology current and would provide a common picture across the entire DoD. Yet if the different cultures of the services continue to do business as usual, the initiative may fail and result in different solutions for every service and agency.

Security Standards for Hardware, Software, and Firmware

A key recommendation is that the nation and DoD must review the quality of the private industry supply chain and develop a means for ensuring hardware, software, and firmware is compliant with established security standards. How can an adequate cyberspace security posture be developed if the hardware, software and firmware that make up the IT infrastructure are flawed with malware? The quality of the hardware, software and firmware is critical, and in many instances has been found to be deficient. In 1998 the Army started the development of an Information Assurance Approved Products List (IAAPL). The concept was simple. For certain Information Assurance (cyber protect) tool categories such as firewall, Intrusion Prevention Systems (IPS), Virtual Private Networks (IPV), to mention but a few categories, Army organizations could only purchase those products that were on the IAAPL. To get on the list the vendor had to meet DoD standards. Any vendor that met the requirements could be on the list. [45] The Army then adds these vendors to Army contracts so as to provide a contract vehicle for Army customers. [46] One may ask, are these standards trivial or important? A prime example of critical standards is that all cryptographic modules are required to receive certification from the National Institute of Standards and technology (NIST). “This certification basically validates that a cryptographic module meets a claimed level of security and that a validated cryptographic algorithm has been implemented correctly”. [47] In 2006 the Computer Security Division of the National Institute of Standards and Technology (NIST) reported that “of the first 200 modules tested, 48 percent of the cryptographic modules and 27 percent of the cryptographic algorithms brought in for voluntary testing had security flaws that were corrected during the testing. In other words, without this program, the government had a 50-50 chance of buying correctly implemented cryptography" [48]

Another reason to have vendors undergo testing to see if security standards are being met is the example of the Seagate hard drives that were produced in Thailand. It was discovered that a piece of the firmware established a connection that terminated in China. [49]

In July 2009 NSS labs performed a test of web browsers to see how they protect against socially engineered malware. The lab tested Internet Explorer 8, Firefox 3, Safari 4, Chrome 2, and Opera 10. The best was Internet Explorer 8 which blocked 81 %of the attacks and the next best performing browser was FireFox 3 that only blocked 27 % of the attacks. The worst performing was a beta browser Opera 10 that only blocked 1 % of the attacks. This is again an example of industry not meeting established standards. [50] The highly publicized Chinese hacker attack against Google in January of 2010 was due to vulnerability in the Microsoft Internet Explorer web browser. [51]

It would be extremely time consuming to validate that the hardware, software and firmware components of a product are free from malware. Thus it would be to the advantage of an attacker to introduce vulnerabilities into the hardware, software and firmware components, long before any attack is executed. [52] The only means of ensuring that hardware, software and firmware are vulnerability free is during the development and manufacturing phase of the supply chain. Based on the significant number of documented software vulnerabilities that are found and the increasing number of hardware flaws that are being publicized, it is clear that industry is not producing commercial products that meet reasonable security standards.

In summary, the increasing evidence of numerous vulnerabilities and malware being discovered in hardware, software and firmware demands that the quality of the supply chain be improved, and a means for ensuring compliance is essential.

Critical Technologies

Another critical initiative that must be undertaken is the establishment of a joint governmental and industry forum that develops and coordinates clear and concise policies and standards for evolving technologies. The cyber protection community is notorious for being reactive rather than proactive. This type of forum, armed with the authority and correct mixture of technicians, policy developers and operational personnel could contribute immensely to the community being more proactive. This forum must be sensitive to the emergence of key IT technologies and develop policies, strategies and standards that can be enforced.

How long has the IT world known about social network technologies? Certainly long enough to have developed policy and standards! Yet as of February 2010 there is no national or DoD policy. The emerging use of social media sites is a technically challenging security risk to the nation and the DOD as well as an invaluable collaborative or marketing resource. Social networking is an ever expanding, wide-ranging definition for the technologies used to share information through ad-hoc or structured communications and connections mostly through the online building of social communities of people who share interests and activities or who are interested in exploring the interests and activities of others. [53] The nature of these sites provides a rich breeding ground for social engineering attacks, phishing, or malicious content to be embedded and executed upon access or download to a DOD protected information system. The dilemma is how to protect the nation and the DoD information systems against this cyber malware vector and yet allow use of this valuable technology. There is an absence of clear guidance on how to proceed. Often there are articles and papers written on the subject, but they fail to adequately address how to balance the risk and value these technologies present. An article written in April 2009 recommends that these technologies be used, but merely acknowledges the issue of security in two short paragraphs with no security specifics. This article articulates a strong case for the use of the technologies, but fails to add any body of knowledge to the security issue which is key to wide spread acceptance and use. [54] The bottom line is that the nation and the DoD are going to use social media networks. Why are there no policies, guidance, tactics, techniques manner that provides adequate security?

Another emerging technology that is starting to be implemented on an enterprise scale is cloud computing, which will serve as the basis of the next generation INTERNET computing environment. In his book the “Big Switch” Nicolas Carr describes the impact that the transition from an organization/company providing their own source of electricity to those same organizations/companies receiving their electricity from large scale power plants that were operated via large utility companies. He states that “the social ramifications of the democratization of electricity would be hard to overstate”. He further states that cheap and plentiful electricity shaped the world we live in today. It’s a world that didn’t exist a mere hundred years ago, and yet the transformation that has played out over a few generations has been so great, so complete, that it has become almost impossible to imagine what life was like before electricity began to flow through the sockets in our walls." [55] He states that we are in the midst of another transformation and it will involve the processing of information. The basis of his book is that companies and even individual computer users will be able to access information from large utility like resources that will enable companies and individuals to access computing power, information and analysis to a degree that will dwarf current capabilities. The "Network is the Computer" is a commonly used phrase that reflects the environment of cloud computing. Instead of being limited to the applications or operating system that is loaded on a personal computer, server farm or data center, the user will now be able to use services that are available from the entire INTERNET. Thus the word "cloud" is used as a physical depiction of services being provided in a transparent manner drawing upon the entire INTERNET or "computing cloud". Cloud Computing can deliver tens of trillions of computations per second in a way that users can tap through the web making supercomputing available to the masses". [56] There are many types of services that are currently being provided and being developed for the "cloud. [57] The main point that needs to be made is that "cloud computing" is still evolving and it is critical that standards for security be established prior to large scale use of commercial "cloud" services and the development of government private, public, hybrid and community deployment models. Due to the fact that services could potentially be delivered from hundreds, if not thousands of hardware/storage platforms, it will be much more difficult to detect and recover from a security breach. If an intruder is found inside the "cloud" it would exacerbate governance issues due to the requirement to report and provide protective services to individuals that may be the victim of a potential or confirmed compromise of Health Insurance Portability and Accountability Act (HIPAA) and Privacy

Act information. There are already articles about intrusions into commercial cloud environments [58] and potential attacks. [59] The National Institute of Standards and Technology (NIST) plans on producing publications on cloud models, architectures, and deployment strategies. Unfortunately, since there will no “watch dog” agency with the authority to establish and enforce standards in the commercial or governmental “cloud” environment, the quality of security will vary significantly. It is foolish to suggest that the way to ensure an adequate security environment is to block cloud computing initiatives. The technology is here to stay, will continue to grow, and is a valuable technology. If this evolving technology is going to provide adequate protection, it cannot be business as usual. If the standards and tools for “cloud” implementations are not established and enforced, the “cloud” environment will retain the same security deficiencies that exist today.

Another key technology that plays an important role in cloud computing is virtualization. “Virtualization is a technology that partitions a computer into several independent machines that can support different operating systems (OS) and applications running concurrently”. [60] “Virtualization refers to a concept in which access to a single underlying piece of hardware, like a server, is coordinated so that multiple guest operating systems can share a single piece of hardware; with no guest OS being aware that it is actually sharing anything at all. The guest OS is an OS that is hosted by the underlying virtualization software layer. A guest OS appears to the application running on it as a complete operating system, and the guest OS is completely unaware that it’s running on top of a layer of virtualization software rather than on the physical hardware” [61] One of the main advantages of virtualization is that it reduces the amount of hardware that is normally needed in a non virtualization environment, thus reducing the cost for space, energy and information technology (IT) support. For these reasons alone, virtualization technology is here to stay, and the nation, as well as the DoD, must learn how to secure the technology. Industry has organized “The Cloud Security Alliance” to research and provide guidance for the secure implementation of not only cloud computing but also the key “cloud” virtualization technology. [62] The Alliance has produced a document entitled Security Guidance for Critical Areas of Focus in Cloud Computing. [63] The Alliance also states that they have aligned their latest guidance version with the National Institute of Standards and Technology (NIST) and their working definition of cloud computing. [64] The Cloud Alliance mentions on numerous occasions that customers must understand, depending upon what services the customer contracts for, the customer may still be responsible for implementing and managing security controls. [65] The document states that while security controls in cloud computing are mostly the same, (no different than many security controls required in a traditional IT environment), technologies used to support cloud services/computing may present different risks than the traditional IT environment. [66] The Alliance discusses the degree of owner responsibility for security again stating “the consumer in turn, is responsible for security controls that relate to the IT system including the operating system, applications, and data. [67] NIST conducted a survey in which security was identified as the number one concern, even more important than performance and availability. It is clear that while virtualization and “cloud” computing introduce innovative technologies and represent the future of IT, the owner still has the responsibility of not only maintaining traditional security controls but to learn about the new risks these technologies will present. [68]NIST intends to develop and publish standards for “cloud” computing and supporting technologies standards for industry and the government, but as of February 2010 this effort consisted of broad general definitions and a large Power Point presentation. [69] As asked previously, who will ensure that the technologies, tools and implementations meet the standards that NIST will publish? How can anyone say that adequate protection is being provided if there is no oversight, no audit?

Summary of Recommendations

The protected and assured use of cyberspace is essential to the national economic well being, social progress and security. The threat to cyberspace is increasing sophisticated and quickly challenging the ability of nation states to provide a stable environment for the use of cyberspace. In this paper there were a number of recommendations that were made so as to facilitate the development of a viable and adequate cyberspace protection posture. In summary, the initial action/recommendation that must be implemented/followed , is that the national leadership needs to educate the private and public sectors about what is going on in cyberspace, the risk it possess to the future of the nation, and the role that all levels of government, the private sector and the individual citizen must execute. Unfortunately the nature of the change that is necessary to develop an adequate protection posture is so radical it may take a cyber disaster to foster an effective response.

Another recommendation is that the nation needs to use all the diplomatic, information, economic, and military elements of influence to forge an international standard that will govern cyberspace through treaties, conventions, laws, and agreements. These efforts will not stop espionage, they will not stop criminal activity, but they would identify these types of activity as being illegal and not acceptable. They would serve as the basis for an adequate degree of predictability in cyberspace.

There must be a national level forum that provides the basis for cooperation between private industry and the appropriate governmental agency to ensure that there is an enterprise approach to protecting cyberspace. Many of the components of the national critical infrastructure operate on an ad hoc basis. Each actor determines how much they share and when. Each actor determines their own level of security. In general they do not operate as an enterprise that shares a common, agreed upon, level of security.

It is important that the security standards for hardware, software and firmware are improved and that a joint industry and governmental forum is established that has the authority to establish and enforce standards. Key hardware, software, and firmware components ought to be required to receive a stamp of approval from this forum. The stamp of approval would indicate that these components were manufactured under conditions and standards that would guarantee a certain level of security. The buyer of key IT components should be able to purchase products that are guaranteed to have met certain security standards.

The final recommendation is that government and industry need to establish a forum that researches and determines what emerging technologies will play a key role in cyberspace, and then establish industry standards and best business practices for that technology. This would apply to social networking technologies as well as virtualization and cloud computing. These are “game changing” technologies that need standards and best business practices to follow when they are first implemented.

These recommendations may seem radical to the point that they are not something that will ever be implemented. They require a level of trust and cooperation not previously seen between government and industry, and will require a level of sophistication not normally associated with the general population. Unfortunately, the nature of the cyberspace challenge will demand this degree of cooperation and sophistication. The United States will have to move towards a degree of shared cooperation that is not normally associated with a capitalist economy. It may be called socialism, governmental interference or "big brother", but this level of cooperation, control and sophistication will become essential if the United States is to maintain a high economic standard, continue to progress socially, and to live in a secure environment.

Endnotes

[1] Robert M. Gates, *Quadrennial Defense Review Report,* (Washington DC: The Secretary of Defense, February 2010) 37.

[2] This type of threat is often referred to as Advanced Persistent Threat (ADT). It is considered advanced because the full spectrum of intrusion technologies and techniques are used. The techniques may in isolation not be advanced but the fact that it is continually monitored and evaluated the methodology is considered advanced. It is considered persistent because the target is continuously attacked and monitored for any weakness/vulnerability until success is achieved. It basically correlates with the accepted fact that anyone can break into anything if they have sufficient tools, expertise, time and intent.

[3] K. Ackerman, "Threats Imperil the Entire U.S. Infrastructure: From the Military to the Economy, the Country is Open to vast Damage," Signal, July 2009, 18-22.

[4] George W. Bush, The National Strategy to Secure Cyberspace (Washington, DC: The White House, 2003)

[5] Dr. Ian Brown and Lilian Edwards, McAfee Virtual Criminology Report 2008: Cyber Crime Versus Cyber Law, 4-9

[6] Lieutenant Commander Matthew J. Sklerov, "Responding to International Cyber attacks as Acts of War," in *Inside Cyber Warfare,* ed. Jeffery Carr (Sebastopol, CA: O'Reilly Media, December 2009), 45-75.

[7] Greylogic, Project Grey Goose "Report on Critical Infrastructure: Attacks, Actors, and Emerging Threats," January 21, 2010, http://www.scribd.com/doc/25550091/Proj-Grey-Goose-report-on-critical-infrastructure-attacks-Actors-and-Emerging-Threats (accessed January 29, 2010).

[8] Ibid., Letter of Introduction

[9] Ibid., 5

[10] Ibid., vii

[11] Paul B. Kurtz, Virtual Criminology report 2009, Virtually Here: The Age of Cyber War, 15-23

[12] Clay Wilson, Botnets, Cyber Crime and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report for Congress RL-32114 (Washington, DC: Congressional Research Service, January 29, 2008), p 8-10.

[13] Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure

[14] Ibid., iii-iv

[15] Ibid., 7-11

[16] "Introducing the new Cyber security Coordinator," December 22, 2009, http://whitehouse.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator (accessed January 29, 2019).

[17] Paul B. Kurtz, Virtual Criminology report 2009, Virtually Here: The Age of Cyber War, 13

[18] Frontline: Cyber war: The Warnings, April 24, 2003, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/

[19] Nathan Thornburgh, The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them), *Time*, August 29, 2005

[20] Simon Elegant, Cyberwarfare: The Issue that China Won't Touch, Time, November 18, 2009

[21] U.S.-China Economic and Security Review Commission, 2009 Report to Congress, (Washington, DC: U.S Government Printing Office, November 2009)

[22] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine*, August 21, 2007,

[23] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., Cyber power and National Security, (Washington, D.C.: National defense University Press, 2009) 525.

[24] Project Grey Goose, “Russia/Georgia Cyber War – Findings and Analysis”, October 17, 2008, http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report (accessed January 29, 2010).

[25] Stephen W. Korns and Joshua E. Kastenberg, “Georgia’s Cyber Left Hook, ”Parameters Volume XXXVIII, no.4 (Winter 2008-2009)

[26] Siobhan Gorman, Yochi J. Dreazen and August Cole, “Insurgents Hack U.S. Drones,” *Wall Street Jounal*, December 17, 2009.

[27] James A. Lewis, “Cyber Attacks and Their Implication for Cyber Conflict”, October 2009, http://csis.org/publication/korean-cyber-attacks-and-their-implications-cyber-conflict, (accessed January 29, 2010).

[28] Ariana Eunjung Cha and Ellen Nakashima, “Google Attack Part of Vast Campaign,” http://www.washingtonpost.com/wp-dyn/content/article/2010/0113/ar2010011300359.html.

[29] Bryan Krekel, “Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation”, October 16, 2009) (accessed December 9, 2009, http://www.uscc.gov.900/.../NorthropGrumman_PRC_Cyber_Paper_Final_approved%20report_16OCT2009.pdf,p 9

[30] Jack Goldsmith, ‘Can We Stop the Cyber Arms Race,” *The Washington Post*, February 1, 2010.

[31] Jeffery Carr, *Inside Cyber Warfare* (Sebastopol, CA: O’Reilly Media, December 2009), 47.

[32] Council of Europe – ETS 185, “Convention on Cybercrime”, 23.XI.2001, http://conventions.coe.int/Treaty/enTreaties/html/185/htm (accessed February 1, 2010).

[33] Computer Crime Research Center, “Putin Defies Convention on Cybercrime,” March 28, 2008,www.crime-research.org/news/28.03.2008/3277/ (accessed February 1, 2010.

[34] Jeffery Carr, *Inside Cyber Warfare* (Sebastopol, CA: O’Reilly Media, December 2009), 47.

[35] Michael N. Schmitt, “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,” June 1999, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471993&Location=U2&doc-GetTRDoc.pdf (accessed February 1, 2010).

[36] Major Graham H. Todd, “Armed Attack In Cyber Space: Deterring Asymmetric Warfare with an Asymmetric Definition,” The Air force Law Review v. 64 (2009): 65-102 (accessed January 4, 2010). Major Arie J Schapp, “Cyber Warfare Operations: Development and use under International Law,” The Air force Law Review v. 64 (2009): 121-173 (accessed January 4, 2010). Lieutenant Colonel Joshua E. Kastenberg, “Changing the Paradigm of Internet access from Government Information Systems: A Solution to the Need for the DoD to Take Time-Sensitive Action on the NIPRNET,” The Air force Law Review v. 64 (2009): 175-209 (accessed January 4, 2010). Lieutenant Colonel Todd A. Brown, “Legal Propriety of protecting Defense

Industrial Base Information Infrastructure," The Air force Law Review v. 64 (2009): 211-257 (accessed January 4, 2010).

[37] EU News, Policy Positions & EU Actors online, "NATO Agrees Common Approach to Cyber Defense", 8 December 2009, http://www.euractiv.com/en/infosociety/nato-agrees-common-approach-cyber-defense/article

[38] U.S. Secretary of Defense Robert M Gates, "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations" memorandum for secretaries of the Military Departments, Washington DC, June 23, 2009.

[39] Ibid., 1.

[40] Some are concerned that the Cyber Command mission may be seen as overlapping or competing with the Homeland Security mission and result in bureaucratic infighting.

[41] Ellen Nakashima, "Google to enlist NSA to Ward Off Attacks," February 4, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03AR2010020304057.html (accessed February 22, 2010).

[42] During the FY10 – FY15 POM process the Army validated $990M dollars of Information Assurance (IA) requirements per year. The Army IA office only received $160M per year.

[43] Defense Information Systems Agency, Host Based Security System (HBSS), http://www.disa.mil/hbss/index.html (accessed December 17, 2009.

[44] Observations based on being an Army representative attending many of the ESSG meetings, reading the minutes for all meeting and then attending as the Army voting member from 1 October 2008 until July 2009.

[45] Army Senior Information Assurance Officer, LeRoy Lundgren, "Letter to Industry Concerning the Approval and Acquisition of Information Assurance (IA) Tools and Products in the United States Army, memorandum to Industry, Washington DC, May 21 2009.

[46] Current COTS and GOTS IA tools, December 4, 2009, https://informationassurance.us.army.mil

[47] With the passage of FISMA, there is no longer a statutory provision to allow for agencies to waive mandatory FIPS. Therefore, except when using National Security Agency approved cryptography, all agencies must use cryptography validated under FIPS 140-2, Security Requirements for Cryptographic Module. This standard specifically requires all hardware, software, and firmware employing cryptography – whether commercial-off-the-shelf or government produced – to be validated through the Cryptographic Module Validation when used for the protection of sensitive unclassified information. Agency acquisition, development, and the use of any hardware, software, or firmware using unvalidated cryptography for the protection of sensitive unclassified information are not permitted and no other validation process can substitute for FIPS validation".

[48] National Institute of Standards and Technology, Computer Security Division 2008 Annual Report, 15.

[49] Reuters, “China Virus Found in Seagate Drives in Taiwan”, November 12, 2007, http://www.reuters.com/article/idUSTP20376020071112

[50] NSSLabs Report, “Web Browser Security: Socially Engineered Malware Protection Comparative Test Results 2ND Edition,” http://www.scribd.com/NSS-Labs-Browser-Security-Phishing-Q3-2009 (accessed February 23, 2010.

[51] Chris Leftkow, “Web Browser Vulnerability used in Google Attacks: Microsoft,” http://news.yahoo.com/s/afp/20100115/tc_afp/uschinaitcompanyinternetgooglemicrosoftmcafee (accessed January 25, 2010).

[52] Wesley K Clark and Peter L. Levin, “Securing the information Highway”,” Foreign Affairs Vol. 88, Issue 6 (Nov /Dec 2009): 4.

[53] Charlene Li and Josh Bernoff, *Groundswell: Winning in a World Transformed by Social Technologies* (Boston Massachusetts: Harvard Business Press 2008), 3-37.

[54] Mark Drapeau and Linton Wells II, “Social Software and National security: An Initial Net Assessment,” April 2009, http://www.ndu.edu/ctnsp//Defense_Tech_Papers.htlm (accessed February 1, 2010).

[55] Nicholas Carr, Big Switch: Rewiring the World, from Edison to Google (New York London: W.W. Norton and Company, 2009), 11-12.

[56] Peter Fingar, *DOT.CLOUD: The 21st Century Business Platform* (Tampa, Florida, USA, 2009), 53.

[57] Ibid, 59

[58] Jolie O’Dell, “Bank Login-Stealing Botnet Found Hiding in Amazon Cloud,” ReadWrite Web, December 10, 2009, http://www.readwriteweb.com/archieves/zeus-botnet-amazon-cloud-ec2.php (accessed December 15, 2009).

[59] Robert McMillian, “Researchers Find a New Way to Attack the Cloud,” IDG News Service, September 3, 2009, http://pcworld.about.com/od/securit1/Researchers-Find-a-New-Way-to.htm (accessed November 11, 2009).

[60] Danielle Ruest and Nelson Ruet, *Virtualization: A Beginner’s Guide* (New York: McGraw Hill Companies,2009), 30

[61] Bernard Golden, *Virtualization for Dummies* (Hoboken, NJ: Wiley Publishing Inc.,2008), 10

[62] Home page for the Alliance

[63] Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1’” http://www.cloudsecurityalliance.org/, (accessed January 25, 2010).

[64] Ibid.,14.

[65] Ibid.,19.

[66] Ibid.,24.

[67] Ibid.,25.

[68] David Talbot, Security in the Ether, Technology Review, February 2010, 36-42.

[69] Peter Mell and Tim Grance, "Effectively and Securely Using the Cloud Computing Paradigm," October 7, 2009, http://csrc.nist.gov/organizations/fissea/2009-conference/presentations/fissea09-pmell-day3_cloud-computing.pdf (accessed February 1, 2010).